US 20180295140A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2018/0295140 A1

LU et al. (43) Pub. Date: Oct. 11, 2018

(54) **DETECTION OF SPOOFED CALL INFORMATION**

(71) Applicant: **Apple Inc.**, Cupertino, CA (US)

(72) Inventors: **Shi LU**, Foster City, CA (US); **Camille CHEN**, Cupertino, CA (US); **Wenping LOU**, San Jose, CA (US); **Wen ZHAO**, San Jose, CA (US)

(21) Appl. No.: **15/480,284**

(22) Filed: **Apr. 5, 2017**

Publication Classification

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/24	(2006.01)
H04W 12/12	(2006.01)
G06F 17/30	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1416*** (2013.01); ***H04L 65/1006*** (2013.01); ***H04L 65/1076*** (2013.01); ***H04L 63/1466*** (2013.01); ***H04L 41/12*** (2013.01); ***H04W 12/12*** (2013.01); ***G06F 17/30864*** (2013.01); ***H04L 65/1069*** (2013.01)

(57) **ABSTRACT**

A mobile device receives an invitation to commence a media session. The invitation may be from a legitimate caller or from a spoofing caller. The mobile device checks parameters using templates to evaluate a consistency of the invitation with respect to a database in the mobile device. The templates include session protocol, network topology, routing, and social templates. Specific template data includes standardized protocol parameters, values from a database of the mobile device and phonebook entries of the mobile device. Examples of the parameters include capabilities, preconditions, vendor equipment identifiers, a hop counter value and originating network information. The originating network information may be obtained from the database by first querying an on-line database to determine a network identifier associated with caller identification information in the invitation. Then, the obtained carrier identifier is used as an index into a database to obtain template data characteristic of the identified originating network.